Komplexitätstheorie

Sommersemester 2020

Mario Holldack, M. Sc.
Prof. Dr. Georg Schnitger
Hannes Seiwert, M. Sc.

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Institut für Informatik
AG Theoretische Informatik

Übungsblatt 3

Ausgabe: 11.05.2020
Abgabe: 18.05.2020

Die Abgabe erfolgt per E-Mail an Mario Holldack (`holldack@em.uni-frankfurt.de`).

Aufgabe 3.1 *SUCCINCT-3-SAT* $((3+3^*)+3 = 6$ Punkte $+\ 3^*$ Extrapunkte)

Die Sprache SUCCINCT-3-SAT ist die Menge aller Schaltkreise C (mit n Quellen), sodass die von C repräsentierte 3-KNF erfüllbar ist. Zeigen Sie:

a) SUCCINCT-3-SAT ist `NEXP`-vollständig.

   Hinweis: Betrachten Sie die KNF zur Simulation einer Turingmaschinenberechnung im Beweis des Satzes von Cook (Satz 6.1 im Skript Theoretische Informatik 1). Zu dieser KNF gibt es eine äquivalente 3-KNF, die nicht wesentlich größer ist, denn es gilt KNF-SAT $\leq_p$ 3-SAT.

b) SUCCINCT-3-SAT liegt nicht in `P`. *Hinweis:* Zeithierarchie-Satz

Aufgabe 3.2 *Die parallele Komplexität regulärer Sprachen* (6 Punkte)

Sei $\Sigma = \{0,1\}$ ein Alphabet und $A = (\Sigma, Q, q_0, \delta, F)$ ein NFA. Entwerfen Sie eine uniforme Schaltkreisfamilie $(S_n : n \in \mathbb{N})$, sodass S_n die Sprache $L(A) \cap \Sigma^n$ akzeptiert. Die Tiefe von S_n soll durch $\mathcal{O}(\log n)$ beschränkt sein, die Größe soll höchstens $\mathcal{O}(n)$ betragen. (Es ist also $L(A) \in \texttt{DEPTH-SIZE}_{\text{uniform}}(\log n, n)$ zu zeigen.) Bestimmen Sie auch Größe und Tiefe Ihrer Schaltkreisfamilie in Abhängigkeit der Zustandszahl $|Q|$.

Hinweis: Verwenden Sie einen Divide & Conquer-Ansatz. Für eine Eingabe $w \in \Sigma^n$ mit $w = uv$ ist die Bestimmung von $q = \hat{\delta}(q_0, u)$ ein naheliegendes Teilproblem. Aber wie kann die Bestimmung von $\hat{\delta}(q, v)$ gleichzeitig ablaufen, ohne dass der Zustand q bekannt ist?

Aufgabe 3.3 *Unbeschränkter Fanin und Blitzgeschwindigkeit* $(3{\times}4 + 4^* = 12{+}4^*$ Punkte)

Manchmal gelingen Konstantzeit-Berechnungen durch „vernünftig große“ Schaltkreise mit unbeschränktem Fanin, aber es gibt auch einfache Probleme, die extrem viele Gatter erfordern.

a) Die Parität von n Bits $\textsc{Xor}_n(x) := x_1 + \cdots + x_n \bmod 2$ sei mit einer DNF zu bestimmen. Zeigen Sie: Es werden mindestens 2^{n-1} Gatter benötigt.

b) Seien $x, y \in \{0,1\}^n$ die Binärdarstellungen der Zahlen $\text{Zahl}(x)$ und $\text{Zahl}(y)$. Konstruieren Sie einen Schaltkreis S_n konstanter Tiefe und polynomieller Größe (in n), der die Binärdarstellung der Summe $\text{Zahl}(x)+\text{Zahl}(y)$ berechnet.

c) Zeigen Sie, dass $2^{\mathcal{O}(\sqrt{n})}$ Gatter genügen, um $\textsc{Xor}_n(x)$ mit einem Schaltkreis der Tiefe drei zu berechnen. (Die Tiefe eines Schaltkreises S ist die Länge eines längsten Weges in S, wobei Negationsgatter nicht mitgezählt werden.)

d) *Bonusaufgabe:* Verallgemeinern Sie die Aussage aus Teil c) für beliebiges $k \in \mathbb{N}$: Entwerfen Sie einen Schaltkreis der Tiefe k und möglichst wenigen Gattern, der $\textsc{Xor}_n(x)$ berechnet.